数理解析研究所講究録
1013 巻 1997 年 60-64

量子相対エントロピーの漸近的達成
Asymptotic Attainment for Quantum Relative Entropy

林 正人 京都大学 数学教室
Masahito Hayashi
Department of Mathematics, Kyoto University, Kyoto 606-01, Japan
e-mail address: masahito@kusm.kyoto-u.ac.jp

Abstract

In this paper I proved that the quantum relative entropy $D(\sigma\|\rho)$ can be asymptotically attained by Kullback Leibler divergences of probabilities given by a certain sequence of measurements. The sequence of measurements depends on ρ, but is independent of the choice of σ.

1 Introduction

In classical statistical theory the relative entropy $D(p\|q)$ is an information quantity which means the statistical efficiency in order to distinguish a probability measure p of a measurable space from another probability measure q of the same measurable space. The states correspond to measures on measurable space. When p, q are discrete probabilities, the relative entropy (called also information divergence) introduced by Kullback and Leibler is defined by [1]:

$$D(p\|q) := \sum_i p_i \log \frac{p_i}{q_i}.$$

In general, when p, q are measures on measurable space Ω, the relative entropy is defined by:

$$D(p\|q) := \int_\Omega \log \frac{dp}{dq}(\omega) p(d\omega),$$

where $\frac{dp}{dq}(\omega)$ is Radon-Nikodym derivative of p with respect to q.

Let $\mathcal{H} := \mathbf{C}^k$ be a Hilbert space which corresponds to the physical system of interest. In quantum theory the relative entropy was first studied by Umegaki [2]. In quantum theory the states of a system corresponds to positive operators of trace one on $\mathcal{H}$. (These operators are called densities.) The quantum relative entropy of a states ρ with respect to another states σ is defined by:

$$D(\sigma\|\rho) := \mathrm{tr}\, \sigma(\log \sigma - \log \rho).$$

States are distinguished through the result of a quantum measurement on the system,. The most general description of a quantum measurement that can be performed on a system is given by the mathematical concept of a completely positive instrument [3] on the system state space. It can be easily shown that for extracting information, it suffices to concentrate on the measurement probability without the need of successive measurements on the already measured system. The most general description of a quantum measurement probability is given by the mathematical concept of a *positive operator valued measure* (POM) [4,5] on the system state space. Generally speaking, if Ω is measurable space, a measurement M satisfies the following:

$$M(B) = M(B)^*, M(B) \geq 0, M(\emptyset) = 0, M(\Omega) = \mathrm{Id} \text{ on } \mathcal{H}, \text{ for any } B \subset \Omega.$$
$$M(\cup_i B_i) = \sum_i M(B_i), \text{ for } B_i \cap B_j = (i \neq j), \{B_i\} \text{ is a countable subsets of } \Omega.$$

A measurement M on $\mathcal{H}$ is called *simple*, if for any $B \subset \Omega$,

$$\int_B M(d\omega)$$

is projection.

$\mathrm{tr}\, M(\cdot)\rho$ denotes the probability by a measurement M on a quantum system $\mathcal{H}$ with respect to a state ρ. An information quantity we can directly access by a measurement M is not $D(\sigma\|\rho)$ but $D_M(\sigma\|\rho)$, where $D_M(\sigma\|\rho)$ denotes $D(\mathrm{tr}\, M(\cdot)\sigma\|\, \mathrm{tr}\, M(\cdot)\rho)$. Because the map $\rho \mapsto \mathrm{tr}\, M(\cdot)\rho$ is the dual of a unipreserving completely positive map [3], by Uhlmann inequality [6] we have

$$D_M(\sigma\|\rho) \leq D(\sigma\|\rho). \tag{1}$$

The equality is attained by a certain measurement M when and only when $\rho\sigma = \sigma\rho$. see for instance [7, Theorem 1.5, Theorem 5.3].

Does the equality of the inequality (1) asymptotically establish? In order to answer the question we define i.i.d. condition.

Let $\mathcal{H}_1, \ldots, \mathcal{H}_n$ be n Hilbert spaces which correspond to the physical systems. Then their composite system is represented by the tensor Hilbert space:

$$\mathcal{H}^{(n)} := \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n = \bigotimes_{i=1}^{n} \mathcal{H}_i.$$

Thus, a state on the composite system is denoted by a density operator ρ on $\mathcal{H}^{(n)}$. In particular if n element systems $\{\mathcal{H}_i\}$ of the composite system $\mathcal{H}^{(n)}$ are independent of each other, there exists a density ρ_i on $\mathcal{H}_i$ such that

$$\rho^{(n)} = \rho_1 \otimes \cdots \otimes \rho_n = \bigotimes_{i=1}^{n} \rho_i.$$

The condition:

$$\mathcal{H}_1 = \cdots = \mathcal{H}_n = \mathcal{H}, \ \rho_1 = \cdots = \rho_n = \rho \tag{2}$$

corresponds to the independent and identically distributed condition (i.i.d. condition) in the classical case. In this paper, we consider under this condition (2) called the quantum i.i.d. condition. The model $\{\rho^{(n)} = \underbrace{\rho \otimes \cdots \otimes \rho}_{n} | \rho \text{ is a state on } \mathcal{H}\}$ is called n-i.i.d. model.

Hiai and Petz proved the following theorem [8].

Theorem 1 *Let ρ, σ be states on $\mathcal{H}$. There exists a simple measurement M_n such that*

$$\frac{D_{M_n}(\sigma^{(n)}\|\rho^{(n)})}{n} \leq D(\sigma\|\rho) \leq \frac{D_{M_n}(\sigma^{(n)}\|\rho^{(n)})}{n} + k\frac{\log(n+1)}{n}. \tag{3}$$

The preceding M_n depends on ρ and σ.

Can we choose a simple measurement M_n satisfying (3) which is independent of σ? The answer is "Yes". The main theorem of this paper is the following theorem .

Theorem 2 *Let ρ be a state on $\mathcal{H}$. There exists a simple measurement M_n such that:*

$$\frac{D_{M_n}(\sigma^{(n)}\|\rho^{(n)})}{n} \leq D(\sigma\|\rho) \leq \frac{D_{M_n}(\sigma^{(n)}\|\rho^{(n)})}{n} + (k-1)\frac{\log(n+1)}{n} for \forall \sigma. \tag{4}$$

2 Simple measurement and quantum relative entropy

In this section we consider the relation between simple measurement and quantum relative entropy. We put some definitions for this purpose. A simple measurement $E(:= \{E_i\})$ is called *commutative* with a state ρ on $\mathcal{H}$ if $[\rho, E_i] = 0$ for any i. For simple measurements E, F, we denote $E \leq F$ if for any i there exists subsets A_i such that $E_i = \sum_{j \in A_i} F_j$. For a state ρ, E_ρ denotes the spectral decomposition of ρ.

Definition 1 *The conditional expectation $\mathcal{E}_E$ with respect to a simple measurement E is defined as:*

$$\mathcal{E}_E : \rho \mapsto \sum_i E_i \rho E_i.$$

Theorem 3 *Let E be a simple measurement. If states ρ, σ are commutative with a simple measurement E and a simple measurement F satisfies that $E, E_\rho \leq F$, then we have*

$$D_F(\sigma\|\rho) \leq D(\sigma\|\rho) \leq D_F(\sigma\|\rho) + \log w(E),$$

where

$$w(E) := \max_i \dim E_i.$$

Note that there exists a simple measurement F such that $E, E_\rho \leq F$.

Proof It is proved by Lemma 1 and Lemma 2. 2

Lemma 1 *Let σ, ρ be states. If a simple measurement F satisfies that $E_\rho \leq F$, then*

$$D(\sigma\|\rho) = D_F(\sigma\|\rho) + D(\sigma\|\mathcal{E}_F(\sigma)). \tag{5}$$

Proof Since $E_\rho \leq F$, F is commutative with ρ. Thus we obtain (5), [9,10]. 2

Lemma 2 *Let E, F be simple measurements such that $E \leq F$. If a state σ is commutative with E, then*

$$D(\sigma\|\mathcal{E}_F(\sigma)) \leq \log w(E). \tag{6}$$

Proof Let $a_i := \operatorname{tr} E_i \sigma E_i, \sigma_i := \frac{1}{a_i} E_i \sigma E_i$. Then $\sigma = \sum_i a_i \sigma_i$ Therefore, from joint convexity of quantum relative entropy [11,12],

$$D(\sigma\|\mathcal{E}_F(\sigma)) \leq \max_i D(\sigma\|\mathcal{E}_F(\sigma_i)) \leq \max_i \log \dim E_i = \log w(E). \tag{7}$$

2

3 Proof of Main Theorem

$Ir^{(n)}$ denotes the simple measurement defined by a irreducible representation of the tensor representation of $\mathrm{GL}(\mathcal{H})$ on $\mathcal{H}^{(n)}$.

Lemma 3 *For any state σ, $Ir^{(n)}$ is commutative with $\sigma^{(n)}$.*

Proof If a state σ is faithful, then it is trivial by Schur's lemma. If a state σ isn't faithful, then there exists a sequence $\{\sigma_i\}$ of faithful states such that $\sigma_i \to \sigma$. Because $\sigma_i^{(n)} \to \sigma^{(n)}$ and $Ir^{(n)}$ is commutative with $\sigma_i^{(n)}$, $Ir^{(n)}$ is commutative with $\sigma^{(n)}$. 2

Theorem 4 *ρ are a state on $\mathcal{H}$. If a simple measurement M_n satisfies that $Ir^{(n)}, E_\rho \leq M_n$, then we obtain the following inequality:*

$$\frac{D_{M_n}(\sigma^{(n)}\|\rho^{(n)})}{n} \leq D(\sigma\|\rho) \leq \frac{D_{M_n}(\sigma^{(n)}\|\rho^{(n)})}{n} + (k-1)\frac{\log(n+1)}{n} \textit{ for } \forall\sigma. \tag{8}$$

Therefore we obtain

$$\lim_{n\to\infty} \frac{D_{M_n}(\sigma^{(n)}\|\rho^{(n)})}{n} = D(\sigma\|\rho) \textit{ for } \forall\sigma.$$

Proof Since $w(Ir^{(n)})$ is the dimension of the k-th symmetric tensor space of $\mathcal{H}$, $w(Ir^{(n)}) = {}_kH_n = \binom{n+k-1}{k-1} = \binom{n+k-1}{n} = {}_{n+1}H_{k-1} \leq (n+1)^{k-1}$, where ${}_kH_n$ denotes the repeated combination of n from k. Therefore, we have $\log w(Ir^{(n)}) \leq (k-1)\log(n+1)$. From Theorem 3 and Lemma 3 we have (8). 2

Note that the simple measurement M_n is independent of σ.

Remark 1 *Even if $\rho_\epsilon \to \rho$ as $\epsilon \to 0$ and M_n satisfies the assumption of Theorem 4, the following equation is not always established:*

$$\lim_{\epsilon\to 0}\lim_{n\to\infty} \frac{D_{M_n}(\rho_\epsilon^{(n)}\|\rho^{(n)})}{n\epsilon^2} = \lim_{n\to\infty}\lim_{\epsilon\to 0} \frac{D_{M_n}(\rho_\epsilon^{(n)}\|\rho^{(n)})}{n\epsilon^2}. \tag{9}$$

Exsample 1 *Let the dimension k of $\mathcal{H}$ be 2. Let us define the Pauli matrices σ_1, σ_2 in the usual way:*

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}.$$

Assume that

$$\begin{aligned} \rho &= \frac{1}{2}(\mathrm{Id} + \alpha\sigma_1), \ 0 < \alpha < 1 \\ \rho_\epsilon &= \frac{1}{2}(\mathrm{Id} + \alpha(\cos\epsilon\sigma_1 + \sin\epsilon\sigma_2)). \end{aligned}$$

then

$$\lim_{\epsilon\to 0} \frac{D_{M_n}(\rho_\epsilon^{(n)}\|\rho^{(n)})}{\epsilon^2} = 0 \tag{10}$$

$$\lim_{\epsilon\to 0}\lim_{n\to\infty} \frac{D_{M_n}(\rho_\epsilon^{(n)}\|\rho^{(n)})}{n\epsilon^2} = \lim_{\epsilon\to 0} \frac{D(\rho_\epsilon\|\rho)}{\epsilon^2} = \frac{1}{4}\alpha\log\frac{1+\alpha}{1-\alpha} > 0 \tag{11}$$

where M_n satisfies the assumption of Theorem 4.

Conclusions

It was proved that quantum relative entropy $D(\sigma\|\rho)$ is attained by a certain sequence of measurements which is independent of σ. This formula is thought to be important for the quantum asymptotic detection and the quantum asymptotic estimation. To know the quantum asymptotic estimation, see [13]. The constructions of these applications are, however, left for future study.

Acknowledgments

I wish to thank to Prof. A. Fujiwara for several discussions on this topic.

References

[1] S. Kullback and R. A. Leibler, Ann. Math. Statist. **22**, 79-86 (1951).

[2] H. Umegaki, Kodai Math. Sem. Rep. **14**, 59 (1962).

[3] M. Ozawa, J. Math. Phys. **25**, 79 (1984).

[4] C. W. Helstrom, *Quantum Detection and Estimation Theory,* (Academic Press, New York, 1976).

[5] A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory,* (North_Holland, Amsterdam, 1982).

[6] A. Uhlmann, Commun. Math. Phys. **54**, 21 (1977).

[7] M. Ohya and D. Petz, *Qunatum Entropy and its Use* (Springer, Berlin, 1993).

[8] F. Hiai and D. Petz, Commun. Math. Phys. **143**, 99-114 (1991).

[9] F. Hiai, M. Ohya and M. Tsukada, Pacific J. Math. **96**, 99-109 (1983).

[10] D. Petz, Acta. Math. Hunger. **47**, 65-72 (1986).

[11] H. Araki, Publ. RIMS, Kyoto Univ. **13**, 173-192 (1977).

[12] H. Kosaki, J. Operator Theory **16**, 335-348 (1986).

[13] M. Hayashi, "Asymptotic estimation theory for a finite dimensional pure state model", submitted Physical Review A.